PIPER MARBURY RUDNICK & WOLFE LLP

1200 Nineteenth Street, N.W.
Washington, D.C. 20036-2412
www.piperrudnick.com

PHONE (202) 861-3900
FAX (202) 223-2085

WRITER'S INFORMATION

paul.jamieson@piperrudnick.com
PHONE (202) 861-6917
FAX (202) 689-7520

August 16, 2001

HAND DELIVERY

Magalie Roman Salas
Secretary
Federal Communications Commission
445 - 12th Street, S.W.
Room TW-A325
Washington, D.C. 20554

Re: Notice of Ex Parte Meetings
CC Docket No. 97-213

Dear Ms. Salas:

This letter is to notify you that on Thursday, August 16, 2001, representatives of the International Softswitch Consortium, Inc. ("ISC"), specifically, Milt Morris, Chairman, ISC Legal Intercept Working Group, Matt Holdrege, Vice Chairman, ISC Legal Intercept Working Group, and Emilio Cividanes, Mark Tauber and I, of Piper Marbury Rudnick & Wolfe LLP, counsel to ISC, met with Monica Shah Desai, Interim Legal Advisor to Commissioner Martin.

The subject of this meeting was ISC's position on the issues in CC Docket No. 97-213 concerning the Communications Assistance for Law Enforcement Act ("CALEA"), including the Petition of the Cellular Telecommunications Industry Association to suspend the September 30, 2001 deadline for compliance with CALEA obligations for packet-mode telecommunications services, as reflected in ISC's filings in the above-referenced proceeding. ISC supports the position that the compliance deadline should be suspended for all packet-switched networks, or, at the very least, for IP packet networks.

Pursuant to 47 C.F.R. § 1.1206(b)(2), an original and two copies of this letter are being provided to you for inclusion in the public record of the above-referenced proceeding. Should you have any questions, please contact the undersigned.

Sincerely,

Paul W. Jamieson

PWJ/eo
Enclosures

cc: Monica Shah Desai
Julius Knapp
Geraldine Matise
Rodney Small
John Spencer

INTERNATIONAL SOFTSWITCH CONSORTIUM POSITION ON CALEA COMPLIANCE DEADLINE FOR PACKET-MODE COMMUNICATIONS

CC Docket No. 97-213
August 14, 2001

I. Background on Organization

The International Softswitch Consortium ("ISC") is a rapidly growing not-for-profit organization working to advance worldwide adoption of next-generation multimedia communications via networks based on packet technologies. The ISC develops open standards, interoperability, and architectures for Internet-based, real-time multimedia and voice applications. Many applications emulate circuit switching in software, hence the name, "Softswitch."

ISC's over 170 member companies, including many of the world's leading communications service providers, equipment vendors and software developers, are at the forefront of a technological and market revolution in the communications service industry.[1] Working groups of the ISC work closely together formally and informally to identify standards, requirements, and solution strategies for the global communications industry. Currently, there are eight working groups established by the ISC's Technical Advisory Council, including the Legal Intercept Working Group, which is developing a safe harbor specification in conjunction with the Federal Bureau of Investigation ("FBI"), pursuant to Section 107(a) of the Communications Assistance for Law Enforcement Act of 1994 ("CALEA"). That safe harbor specification is based on the PacketCable Electronic Surveillance Specification published by Cable Television Laboratories, Inc., but is focused on Softswitch architectures.

II. What Issues Are at Stake for ISC Members

A. Procedural Context

In its *Third Report and Order*,[2] the Commission adopted technical requirements for wireline, cellular and broadband PCS carriers to comply with the assistance capability provisions of CALEA. Specifically, the Commission required carriers to implement all capabilities of the J-STD-025 (the "Interim Standard") and six of the nine "punch list" capabilities requested by the U.S. Department of Justice and FBI by September 30, 2001. The Commission also left in place the September 30, 2001 compliance deadline for packet-mode communications, even as it acknowledged that "the approach taken to packet-mode communications in [the Interim

---

[1] *See* http://www.softswitch.org/asp/memberlist.asp?page=memberlist for a list of current ISC members.

[2] *Communications Assistance for Law Enforcement Act, Third Report and Order,* 14 FCC Rcd 16794 (1999) *("Third Report and Order").*

Standard] raises significant technical and privacy concerns," and invited the Telecommunications Industry Association ("TIA") to report to the Commission on the issue by September 30, 2000.[3]

On August 15, 2000, responding to consolidated petitions for review of the *Third Report and Order* challenging four of the six "punch list" items and inclusion of the packet-mode data requirement in the Interim Standard, the U.S. Court of Appeals for the District of Columbia Circuit vacated and remanded certain portions of the *Third Report and Order*.[4] Specifically, the court found that the Commission's decision to include the four challenged "punch list" items reflected a lack of reasoned decisionmaking, and remanded those sections of the *Third Report and Order* addressing those four "punch list" items. The court upheld the Commission's inclusion of packet-mode data in the Interim Standard, but clarified that carriers do not have to deliver an entire packet stream to a law enforcement agency ("LEA") on a pen register order.[5] As of August 13, 2001, the Commission had not issued an order on remand.

On September 15, 2000, the Cellular Telecommunications Industry Association ("CTIA") petitioned the Commission to suspend the September 30, 2001 compliance date for packet-mode communications.[6] The CTIA Petition explained the uncertainty among affected industry participants that the rapidly approaching September 30, 2001 deadline has engendered.[7] The Petition also explained the difficulty of disentangling the vacated features from the two unchallenged "punch list" items, and the uncertainty around treatment of packet-mode communications after the D.C. Circuit clarified that carriers could not lawfully deliver the full packet content to a LEA on a pen register order.[8] The Commission invited public comment on the CTIA Petition,[9] and several interested parties, including the TIA[10] and ISC,[11] have filed

---

[3] *Id.* at ¶ 55.

[4] *United States Telecom Association, et al., v. FCC,* 227 F.3d 450 (D.C. Cir. 2000). The four vacated "punch list" items are: (1) post-cut-through dialed digit extraction; (2) party hold/join/drop information; (3) subject-initiated dialing and signaling information; and (4) in-band and out-of-band signaling. The two "punch list" items adopted in the *Third Report and Order* but not challenged in the Court of Appeals are the content of subject-initiated conference calls and timing information.

[5] 227 F.3d at 465.

[6] Petition to Suspend Compliance Date of the Cellular Telecommunications Industry Association, CC Docket No. 97-213, filed August 23, 2000 (the "CTIA Petition").

[7] *Id.* at 4-5.

[8] *Id.* at 5-6.

[9] *Comment Invited on CTIA Petition to Suspend CALEA Compliance Date*, DA 00-2022 (released Sept. 1, 2000).

[10] Comments of the Telecommunications Industry Association, CC Docket No. 97-213, filed September 15, 2000.

[11] Letter from Emilio Cividanes, counsel for International Softswitch Consortium, to Dorothy Atwood, Thomas J. Sugrue and Bruce Franca, CC Docket No. 97-21, filed May 24, 2001.

supportive comments. As of August 13, 2001, the Commission had not acted on the CTIA Petition.

On September 29, 2000, TIA submitted its Report on Surveillance of Packet-Mode Communications to the Commission (the "TIA Report"), consistent with the time line of the Commission's request in the *Third Report and Order*. The substantive conclusions and implications raised in the TIA Report are discussed in II.C., below.

B. Softswitch Protocols and Architectures

At the outset, the unique character of Softswitch protocols and architectures must be recognized. Softswitch technology relies on Internet Protocol ("IP") packets for the transmission of both data and voice content. Unlike the Public Switched Telephone Network, packets are transmitted over Softswitch-controlled networks on a connectionless basis. That is, individual packets can flow over any path, without regard to the routing of the previous or subsequent packets. Accordingly, there is no single point in the core of a Softswitch-controlled network where a complete transmission can be intercepted.

Moreover, Softswitch technologies enable implementation of fully distributed networks with no centralized control, and intercepting transmissions at their source undermines the purposes of the interception, since the interception can be detected by the target and others participating in the transmission. Thus, it is necessary to provide for the interception of transmissions at the various points where they enter the core network. The critical problem is, however, that in a variety of Softswitch architectures, providing for such interception is difficult and costly.

As set out in the Attachment hereto, the interception must be provided for in a myriad of devices at the edges of the core networks, not a single or limited number of points within the core. Today, the devices in such networks do not provide intercept capabilities sufficient to comply with CALEA. Those devices will have to be replaced with new devices that provide such capabilities, and all new devices will have to be designed to include such capabilities. In light of the costs involved, the Commission should carefully consider whether the replacement of existing devices should be required and whether there should be limitations on the installation of new devices throughout packet networks. Nevertheless, the Legal Intercept Working Group of the ISC is proceeding, in collaboration with the FBI and other standard-setting bodies, to develop a safe harbor specification for Softswitch technologies. The ISC hopes to publish its safe harbor specification prior to January 1, 2002.

The problem is exacerbated by the fact that the Commission has not yet ruled on the remand of the punch list items by the D.C. Circuit. The design or redesign and the installation of the necessary equipment will be costly and challenging enough once it is clear precisely what capabilities will be required. Being required to do that work multiple times would be an undue burden that would retard or preclude the timely development and implementation of new technologies and services.

C. TIA Report on Surveillance of Packet-Mode Communications

1. Packet-Mode Services Are Extremely Varied and Diverse. Quoting the Commission's *Third Report and Order,* TIA observed that packet technologies are rapidly changing, and different technologies may require differing CALEA solutions for separating call-identifying information from call content.[12] TIA suggested that "it may be appropriate for the Commission to encourage separate standards for each, individual packet technology (for example, PacketCable's standard for packetized cable telephone)."[13]

The ISC agrees that packet technologies are rapidly changing, and that the standards need to be tailored to individual packet technologies. In important respects, there are substantive differences in the architectures and protocols of the technologies. However, there also are substantial similarities in parts of the technologies (*e.g.,* PacketCable and Softswitch technologies). Accordingly, ISC recommends that the September 30, 2001 deadline for packet-mode technologies to meet CALEA requirements should be extended to allow for the continued development of safe harbor specifications which accommodate both the differences and similarities of various packet technologies. ISC is actively working on the development of such specifications for the Softswitch technologies.

2. Technical Difficulty of Analyzing Packet Data Traffic. TIA observes that "[i]t is not technically feasible to determine, on a packet-by-packet basis, the application or service that is being provided in a particular packet stream. Encapsulation (i.e., wrapping packets within packets) and encryption of packets renders identification of the type of service being conveyed (e.g., communications vs. information) even more difficult, if not possible."[14] The ISC agrees with this observation, which underscores the difficulty of compliance with the current packet-mode deadline and the need for additional time to develop an appropriate safe harbor.

3. Most Cost-Efficient and Technically-Feasible Solution. TIA noted that providing the entire packet stream for a particular subscriber is by far the most cost-effective and technically feasible method for providing access to law enforcement. Of course, in order to address privacy concerns, law enforcement must obtain the appropriate legal authorization to receive this packet stream (such as a Title III order) and strict legal procedures should be adopted to assure compliance with the limits on that authorization."[15] In light of that, TIA concluded that requiring carriers to develop a filtering program would be "extremely burdensome and expensive" and, in

---

[12] Letter accompanying the TIA Report from Matthew J. Flanigan and Grant Seiffert to William E. Kennard, September 29, 2000, at 1.

[13] *Id.* at 2.

[14] *Id.* at 3

[15] *Id.* at 4.

any event, that feasibility "will vary from technology to technology and would require individual standards."[16]

The ISC agrees with the privacy and procedural concerns raised by TIA, and that requiring carriers to develop or apply a filtering program would be costly, burdensome, and contravene statutory goals. In any event, ISC agrees that technology-specific standards would need to apply. More time will allow carriers, the Commission and the FBI to develop standards that satisfy CALEA's mandates, while not imposing extraordinary costs on a nascent industry.

4. Call-Management Service. TIA suggested that the point where a Call Management Service ("CMS"):

> sets up a communication may be the only time that a packet-mode communications service can be distinguished from an information service and that call-identification-like information might be identified. Again, however, what might be feasible will vary widely from CMS-technology to CMS-technology. For transport services without a CMS, it is extremely burdensome to segregate individual packets out of the stream of packets being conveyed by the transport carrier and extract the kind of information law enforcement is requesting. In those transport technologies, where the whole packet stream must be examined in order to gather relevant call-identification-like information, the process of filtering may overload the network's processing capacity or severely degrade network performance.[17]

The packet-mode deadline raises significant compliance problems, from maintaining security over legal intercepts (so the target is not aware of the intercept) to providing filtering of *all* packets being transmitted over the network. The Commission's ruling on the remand of the punch list items should confront and resolve these matters, and the deadline should be extended to allow the industry a reasonable opportunity to develop an appropriate safe harbor specification.

5. FBI's Carnivore Presentation. TIA observed that the FBI's "Carnivore" presentation verified that the development of a filter protocol such as Carnivore is extremely resource intensive, and raised the question whether "it would be cost-effective (or even privacy-protective) to require carriers to develop their own, separate capabilities. "[18]

The ISC agrees that the use of Carnivore or any similar system raises far-reaching privacy issues and, depending on the manner in which is was applied, could result in significant costs, as well as network degradation. The ISC is working with the FBI to address these

---

[16] *Id.*

[17] *Id.* at 3.

[18] *Id.* at 4.

concerns. The packet-mode compliance deadline should be extended to allow the Commission to consider the far-reaching implications of any filtering requirement, and for the industry to have time reasonably to implement the Commission's ruling The Commission should take great care to implement CALEA in a manner that does not impose undue costs on carriers.

III. Rationale for Suspension

A. Suspension of the September 30, 2001 Deadline is Required by the Statute and the D.C. Circuit's Decision.

Section 107(b)(2) of CALEA specifies five goals that any Commission-imposed standards formulated in response to challenges to industry standards must meet: (1) compliance with Section 103 through cost-effective methods; (2) protection of the privacy and security of communications outside CALEA's scope; (3) minimization of costs of compliance on residential ratepayers; (4) encouragement of new technologies and services; and (5) provision of a reasonable time and conditions for compliance with and the transition to any new standard.[19]

Failure to suspend the September 30, 2001 deadline for packet-mode technologies would contravene these goals. First, as described above and in the TIA Report, the nature of packet-mode communications will dramatically increase the costs of compliance for ISC members. As Cisco pointed out, an ISP placing a voice-over-IP call made from a PC will typically process only the IP protocol header, and is otherwise unaware that a voice communication is being initiated.[20] Requiring ISPs and equipment manufacturers to recognize that a voice call is being made would require significant and expensive upgrades of network equipment. When this expense is incurred to comply with what the Commission views as a temporary solution for packet-mode technologies, its cost effectiveness is all the more questionable.

Second, it is not clear that the Interim Standard's treatment of packet-mode technologies protects the privacy and security of communications outside CALEA's scope. The Commission recognized in the *Third Report and Order* that application of the Interim Standard to packet-mode technologies would result in LEAs receiving both call-identifying information and call content, "even in cases where a LEA is authorized only to receive call-identifying information."[21] But the D.C. Circuit clarified that this result would violate Section 103.[22] Particularly where an agreed upon definition of "call-identifying information" for IP packet-mode technologies does not exist, application of the September 30, 2001 deadline ill serves carriers who must try to comply with the *Third Report and Order* while not contradicting the D.C. Circuit's mandate.

---

[19] 47 U.S.C. § 1006(b).

[20] Comments of Cisco Systems, Inc., filed December 8, 2000.

[21] *Third Report and Order* at ¶ 55.

[22] 227 F.3d at 465.

Finally, the imposition of the Interim Standard the Commission itself admits is not ideal, coupled with the uncertainty of the punch list items, plainly suggest that the Commission has not provided a reasonable time or conditions for compliance with its standard. It would be unreasonable for the Commission to expect compliance with the September 30, 2001 deadline in the face of this uncertainty.

B. A Suspension of the September 30, 2001 Compliance Deadline Is Consistent with Analogous Commission Actions.

Sections II.B., II.C. and III.A., above, demonstrate that suspension of the September 30, 2001 compliance date for packet-switching technologies is necessary for ISC to develop an appropriate document pursuant to CALEA's safe harbor provision, and in light of the D.C. Circuit's remand of four of the "punch list" items. But a suspension would also be consistent with Commission precedent in analogous situations in which the Commission has postponed a regulatory deadline to give affected parties and the Commission itself an opportunity to address implementation in a cooperative manner and to better give effect to statutory and policy goals.

For example, in adopting technical standards for the display of closed captions on digital television receivers, pursuant to the Television Decoder Circuitry Act of 1990, the Commission granted set manufacturers an additional year beyond the date proposed in the Notice of Proposed Rulemaking for compliance with installation of a decoder.[23] The Commission stressed that the additional year from the adoption of final rules would give industry participants time to comply and would serve both policy and statutory goals of producing reliable equipment. Similarly, the Commission granted substantial extensions to carriers in the face of industry complaints that compliance by the original deadlines for the Emergency 911 rules would be impractical.[24] These extensions were granted to accommodate a broader range of technical options for compliance with the automatic location identification mandates of the E911 rules.[25]

Even in the case of spectrum auctions, for which the Commission is under statutory deadlines to deposit proceeds in the U.S. Treasury, the Commission has delayed deadlines in response to industry concerns and where such delay would better serve the overall statutory goals of putting spectrum to the highest valued use, increasing auction revenues and maximizing spectral efficiency. For example, when potential bidders urged the Commission to delay auction of spectrum in the 700 MHz bands because of concerns over the value of encumbered spectrum

---

[23] *Closed Captioning Requirements for Digital Television Receivers,* 15 FCC Rcd 16788, ¶ 72 (2000).

[24] *See Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems,* 14 FCC Rcd 17388 (1999) (extending dates for complying with certain E911 Phase II requirements).

[25] *Id.* at ¶ 36.

and new package bidding rules,[26] the Commission responded by postponing the auction, citing the need for bidder preparation and for auction administration.[27]

While the examples cited above involve regulatory delays, similar rationales support a suspension of the September 30, 2001 CALEA compliance date for packet-mode technologies. Indeed, the case for suspension of CALEA requirements for packet-mode technologies is much stronger. The Commission has yet to issue an order on remand regarding the vacated "punch list" items, which are inextricably linked to the treatment of packet-switching technologies. Further, the Commission has not responded to the CTIA Petition or the TIA Report that the Commission itself requested. Given that Congress specified a significant industry role in the development of a safe harbor in Section 107, that the Commission itself recognized in the *Third Report and Order* that the Interim Standard's approach to packet-switching technologies "raises significant technical and privacy concerns" and that its solution was not a perfect one,[28] it is unreasonable for the Commission to keep the September 30, 2001 deadline in place, while these matters remain pending. Indeed, a suspension will better serve the statutory goals by providing industry a meaningful opportunity to devise a workable solution to the application of CALEA requirements to packet-mode technologies.

IV. Conclusion

For the aforementioned reasons, the ISC urges the Commission to suspend the September 30, 2001 CALEA deadline for packet-mode technologies.

---

[26] *See, e.g.,* Letter from John T. Scott, Verizon Wireless, to Thomas J. Sugrue, filed January 18, 2001.

[27] *Auction of Licenses for the 747-762 MHz Bands Postponed Until September 12, 2001,* DA 01-266 (released Jan. 31, 2001).

[28] *Third Report and Order* at ¶¶ 55-56.

ATTACHMENT A

International Softswitch Consortium Legal Intercept Scenarios

This document attempts to describe several planned VoIP architectures that are being developed within the ISC for use by telecom operators. The document shows diagrams of each architecture and describes how legal intercept might be performed. This document shall also attempt to describe how legal intercept requirements may or may not stunt the growth of alternative IP telecommunications networks.

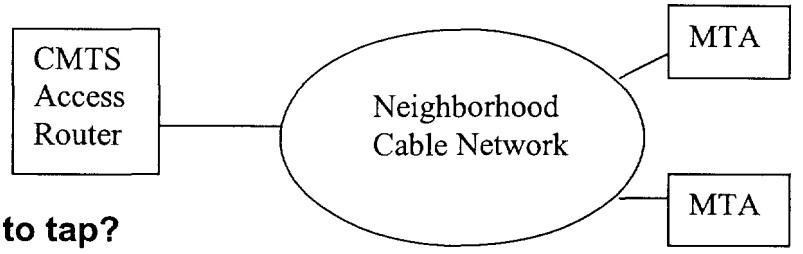
IP Packets versus traditional voice carriers

Traditional voice carriers such as Pulse-Coded Modulated (PCM) speech transported over Time Division Multiplexed (TDM) circuits are fixed in nature. Internet Protocol (IP) packets are connectionless which means they can flow over any path without regard for how the previous or following packet was routed. This makes the concept of intercepting speech very difficult in an IP world. In general, there is no single point in the core of the network where you can place a wiretap and hope to capture a conversation. Of course, you cannot tap at the source or destination without the awareness of the target. So you must try to tap at the Access to the IP core. In some VoIP architectures, this is possible and in others it is extremely difficult and tremendously costly.

The Internet and IP networks have flourished primarily due to the free and flexible nature of IP packets. By attempting to arbitrarily place legacy regulatory requirements on VoIP networks, we may limit the growth of such networks and consequently limit the public benefits. Therefore we wish to attempt to satisfy the pubic needs of lawful intercept (and emergency calling) without impacting the free growth of IP communications. Further we wish to satisfy the above needs without introducing new security holes in IP networks. Lawful Intercept facilities must be protected themselves from unlawful use by so called "hackers". Related information can be found in the Internet Engineering Task Force (IETF) publication known as RFC 2804 located on the Internet at http://www.ietf.org/rfc/rfc2804.txt

We should also mention that the pen register and trap and trace CALEA applications are easily supported in any commercial IP network, purely because accurate usage billing is a requirement. All that remains is to develop or adopt a LEA interface to the billing system to obtain the records. The ISC will work on standardizing such an interface, however billing systems remain mostly proprietary today and the Operator will likely have to satisfy pen register and trap & trace on his own.

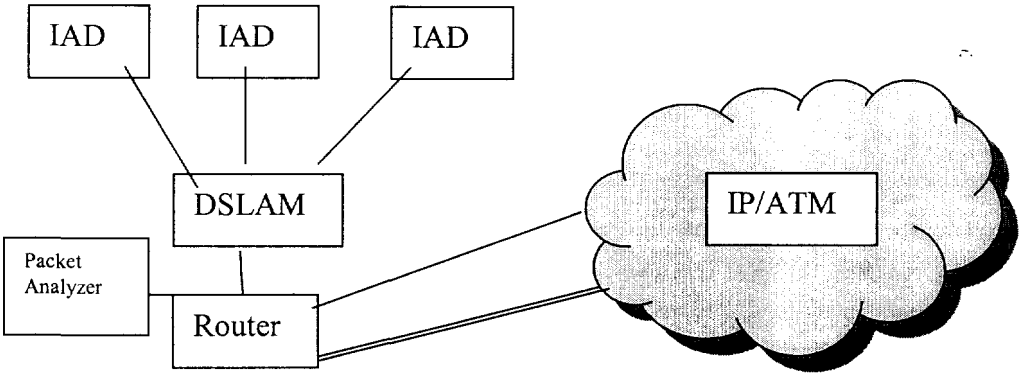
Scenario 1. Cable networks



Where to tap?

- At the CMTS (Cable Modem Termination System). This is the single point of IP access for the Cable Modem (user CPE) and it is defined as a specialized new device that has the characteristics that allow for Lawful Intercept.

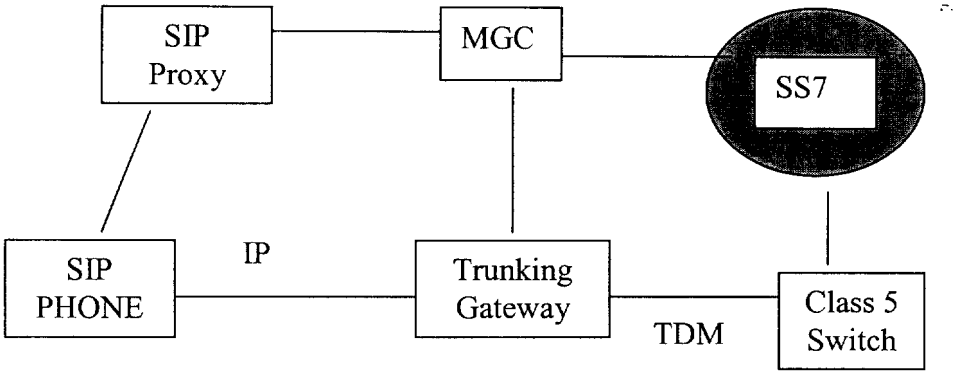
Scenario 2. VoDSL networks



Where to perform intercept?

- At the DSLAM Access router?
  - Would have to upgrade 1000's of routers and each DSLAM could have multiple access routers.
- At the DSLAM?
  - Some DSLAM's are not architected to intercept IP packets. Huge costs involved as DSLAM's are at each C.O. and come in a wide variety of flavors.
- At the IAD?
  - It's CPE and out of bounds for LI
- At the Packet Analyzer?
  - Would mean adding a packet analyzer in front of every access router. The Packet analyzer would have a safe harbour LEA interface meeting the J standard. The LEA interface would query the MGC to find the IP address that matched the target E.164 number. Then the LEA interface would direct the packet analyzer to copy all packets from the target IP address and forward them to the LEA.

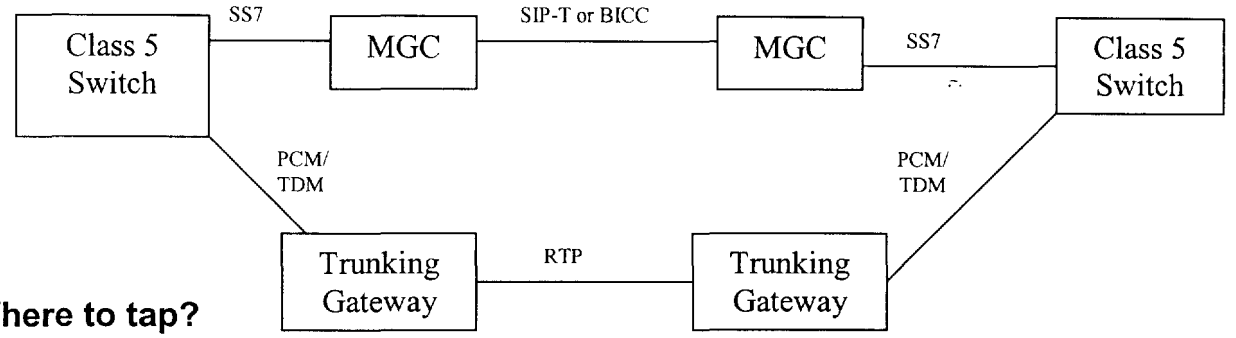
Scenario 3. SIP to PSTN Gateway



Where to tap?

- At the Trunking Gateway?
  - Today's Trunking Gateways do not have the DSP technology to handle LI.
- At the Access Router (not shown)
  - Each IP element may have multiple paths to it's IP Neighbor. A different path could be chosen on a packet by packet basis making it virtually impossible to tap meaningful conversations.
- At the Class 5 switch?
  - This would work, however the Class 5 switch may be in another jurisdiction or country than the target user.

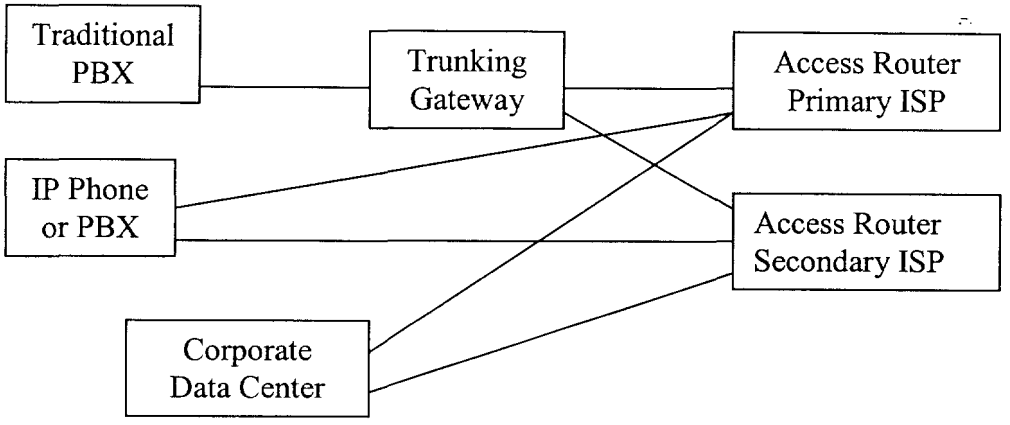
Scenario 4. Tandem Trunking



Where to tap?

- At the Class 5 switch?
  - Yes! While there could be some complex architectures, policies and procedures exist to perform LI at any class 5 switch, even in an international scenario.

Scenario 5. Corporate networks



Where to tap?

- At the Access router?
  - There may be multiple access routers and they may be dealing with a massive amount of data as the corporation may share the same IP pipe for both telephony and data processing. Both issues make it nearly impossible to tap a meaningful flow of IP packets.
- At the Class 5 switch (not shown)
  - Yes, but the Class 5 switch may be located in another jurisdiction or country than the target user. Also, the call might go to an IP user so there would be no Class 5 switch involved.